EXHIBIT KK

TO DECLARATION OF S. MERRILL WEISS IN SUPPORT OF PLAINTIFF ACACIA MEDIA TECHNOLOGIES CORPORATION'S MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO ROUND 3 DEFENDANTS' MOTION FOR SUMMARY JUDGMENT OF INVALIDITY UNDER 35 U.S.C. § 112 OF THE '992, '863, AND '702 PATENTS; AND SATELLITE DEFENDANTS' MOTION FOR SUMMARY JUDGMENT OF INVALIDITY OF THE '992, '863, AND '720 PATENTS

Hovsepian v. Apple, Inc.

Doc. 325 Att. 39

Dockets.Justia.com

J Soc. Indust. Appl. Math.
Vol. 8, No. 2, June, 1960
Printed in U.S.A.

POLYNOMIAL CODES OVER CERTAIN FINITE FIELDS*†

I. S. REED AND G. SOLOMON‡

Introduction. A code is a mapping from a vector space of dimension m over a finite field K (denoted by $V_m(K)$) into a vector space of higher dimension $n > m$ over the same field ($V_n(K)$). K is usually taken to be the field of two elements Z_2, in which case it is a mapping of m-tuples of binary digits (bits) into n-tuples of binary digits. If one transmits n bits, the additional $n - m$ bits are "redundant" and allow one to recover the original message in the event that noise corrupts the signal during transmission and causes some bits of the code to be in error. A multiple-error-correcting code of order s consists of a code which maps m-tuples of zeros and ones into n-tuples of zeros and ones, where m and n both depend on s, and a decoding procedure which recovers the message completely, assuming no more than s errors occur during transmission in the vector of n bits. The Hamming code [1] is an example of a systematic one bit error-correcting code. We present here a new class of redundant codes along with a decoding procedure.

Let K be a field of degree n over the field of two elements Z_2. K contains 2^n elements. Its multiplicative group is cyclic and is generated by powers of α where α is the root of a suitable irreducible polynomial over Z_2. We discuss here a code E which maps m-tuples of K into 2^n-tuples of K.

Consider the polynomial $P(x)$ of degree $m - 1$

$$P(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1},$$

where $a_i \in K$ and $m < 2^n$. Code E is the mapping of the m-tuple $(a_0, a_1, \cdots, a_{m-1})$ into the 2^n-tuple $(P(0), P(\alpha), P(\alpha^2), \cdots, P(1))$; this m-tuple might be some encoded message and the corresponding 2^n-tuple is to be transmitted. This mapping of m symbols into 2^n symbols will be shown to be $(2^n - m)/2$ or $(2^n - m - 1)/2$ symbol correcting, depending on whether m is even or odd.

A natural correspondence is established between the field elements of K and certain binary sequences of length n. Under this correspondence, code E may be regarded as a mapping of binary sequences of mn bits into binary sequences of $n2^n$ bits. Thus code E can be interpreted to be a systematic multiple-error-correcting code of binary sequences.

* Received by the editors January 21, 1959 and in revised form August 26, 1959.

† The work reported here was performed at Lincoln Laboratory, a technical center operated by Massachusetts Institute of Technology with the joint support of the Army, Navy and Air Force, under contract.

‡ Staff members, Lincoln Laboratory, Massachusetts Institute of Technology, Lexington 73, Massachusetts.

One should note that the binary representation of code E allows in general for the correction of more than $(2^n - m - 1)/2$ bits since each symbol of the code is represented by n consecutive bits. Hence when the binary errors are strongly correlated or occur in "bursts," this code may be more desirable than other more "efficient" multiple-error-correction codes.

Finally, it should be mentioned that code E may be generalized to polynomials of the mth degree in several variables over K. Evidently, for $K = Z_2$, such codes reduce to Reed-Muller codes [2].

The code E. Consider the field $K = Z_2(\alpha)$. This is the vector space over Z_2 with basis $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$, where α is the root of a suitable irreducible polynomial over Z_2. The nonzero elements of K form a multiplicative cyclic group. Thus we may represent the elements of K in the order

$$0, \beta, \beta^2, \cdots, \beta^{2^n-2}, \beta^{2^n-1} = 1$$

where β is a generator of the multiplicative cyclic group.

Let $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1}$. The code E sends

$$(a_0, a_1, \cdots, a_{m-2}, a_{m-1}) \to (P(0), P(\beta), P(\beta^2), \cdots, P(\beta^{2^n-2}), P(1)).$$

Upon receiving the message $(P(0), P(\beta), \cdots, P(1))$, we may decode the message by solving simultaneously any m of the 2^n equations,

$$\begin{aligned} P(0) &= a_0 \\ P(\beta) &= a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{m-1}\beta^{m-1} \\ P(\beta^2) &= a_0 + a_1\beta^2 + a_2\beta^4 + \cdots + a_{m-1}\beta^{2m-2} \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ P(1) &= a_0 + a_1 + a_2 + \cdots + a_{m-1}. \end{aligned}$$

We note that any m of these equations are linearly independent since the coefficient determinant for, say, $P(\alpha_1), \cdots, P(\alpha_m)$, is

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{m-1} \\ & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{m-1} \end{vmatrix}$$

which is a Vandermonde determinant whose value is

$$= \prod_{j<i} (\alpha_1 + \alpha_j) \neq 0.$$

Thus in the case of no errors in the received values of $P(\cdot)$, we obtain $\binom{2^n}{m}$ determinations of $(a_0, \cdots, a_{m-1})$.

Exhibit KK Page 062

Any errors occurring in the values of $P(\cdot)$ will immediately disturb the unanimity of the values obtained for the a_n's. Indeed, for sufficiently small numbers of errors, by looking at the largest number of determinations for any $(a_0, \cdots, a_{m-1})$ (the plurality of votes received by any m-tuple) we may detect the order of error made and correct it. We prove the following statement.

Lemma. For s errors we can get at most $\binom{s+m-1}{m}$ determinations for a wrong m-tuple.

Proof. We look upon the simultaneous solution of m equations as the intersection of m hyperplanes. The linear independence guarantees that they meet at only one point. To obtain more than one solution for any m-tuple, we would need more than m hyperplanes meeting at that point. For a wrong m-tuple, we can have at most $s + m - 1$ hyperplanes intersecting at a single wrong point, where s is the number of mistaken equations and where the remaining $m - 1$ equations are chosen from the $2^n - s$ correct ones. Any more correct hyperplanes would determine the correct solution, i.e., a different point of intersection from the assumed wrong one. Therefore, there are at most $\binom{s+m-1}{m}$ determinations for any wrong value. Note that we get $\binom{2^n-s}{m}$ determinations for the correct one, and a total of $\binom{2^n}{m} - \binom{2^n-s}{m}$ wrong determinations.

Thus, by examining the vote received by the individual candidates $(a_0, \cdots, a_{m-1})$, we may determine the correct message and the number s.

Note that this is valid only when

$$\binom{2^n-s}{m} > \binom{s+m-1}{m}$$

or

$$2^n - s > s + m - 1$$

or

$$s < \frac{2^n - m + 1}{2}.$$

The code will thus correct errors of order less than $(2^n - m + 1)/2$. For m odd, we get corrections up to $s = (2^n - m - 1)/2$, and detection at $s = (2^n - m + 1)/2$. For m even, we can correct up to $s = (2^n - m)/2$ and not detect any further errors.

Translation of K into a binary alphabet. We represent the elements of K by n-tuples of zeros and ones, $V_n(Z_2)$, and define a multiplication on $V_n(Z_2)$ corresponding to the multiplication of K. We again note that the multiplicative group of K is generated by powers of β. Let us consider an irreducible polynomial f which generates K over Z_2. Suppose $f(x) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n = 0$, $c_i \in Z_2$. Following N. Zierler [3], we associate the following finite difference equation

$$a_{n+k} + c_1a_{n-1+k} + c_2a_{n-2+k} + \cdots + c_na_{0+k} = 0$$

where $a_i \in Z_2$.

Thus for any fixed f (giving rise to $(c_1, \cdots, c_n)$) and arbitrary $(a_0, \cdots, a_{n-1})(a_i \neq 0$ for $i = 0, 1, \cdots, n-1)$ we have a sequence

$$a_0, a_1, \cdots, a_{n-r}, a_n, a_{n+1}, a_{n+2}, \cdots$$

where the values of a_i for $i \geqq n$ are determined by the above difference equation. Zierler has shown that for suitable irreducible f, the sequence (a_n) is periodic of period $2^n - 1$, i.e., $a_{2^n-1} = a_0$, $a_{2^n+m-1} = a_m$ and the $2^n - 1$ sequences of length n obtained by translating the n-tuple $(a_0, a_1, \cdots, a_{n-1})$ along the derived sequence are all distinct.

Thus if we define

$$\beta = (a_0, \cdots, a_{n-1})$$
$$\beta^2 = (a_1, \cdots, a_n)$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$\beta^m = (a_{m-1}, \cdots, a_{n+m-2})$$

we have a multiplication table for the n-tuples. In other words, multiplication of the elements is simply translation along this periodic sequence generated by f. Note too that the elements β satisfy the algebraic equations satisfied by corresponding elements in K. We have thus defined multiplication on $V_n(Z_2)$ to make this correspond with the multiplication on K.

We remark that the initial choice of $\beta = (a_0, \cdots, a_{n-1})$ is arbitrary and there are $2^n - 1$ such representations. There are of course many other ways of associating vectors with powers of β. The referee has suggested another natural algebraic association of $V_n(Z_2)$ with K.

We identify K with the ring of polynomials in x with coefficients in Z_2, (i.e., $Z_2[x]$) modulo the prime ideal generated by the irreducible $f(x)$. Let $\beta = (a_0, a_1, \cdots, a_{n-1})$ be a nonzero vector of $V_n(Z_2)$. We associate with β the polynomial $\beta(x) = a_0 + a_1x + a_2x^2 + \cdots a_{n-1}x^{n-1} \bmod f(x)$. Consider $\beta(x)^k \bmod f(x)$. This again is a polynomial of formal degree $(n-1)$. Let β^k be the vector whose components are the n coefficients of this $(n-1)$-degree polynomial. This establishes a one-one correspondence of $V_n(Z_2)$

with K(if $(0, 0, \cdots, 0)$ is added to correspond to zero in K). While this may be a more natural choice, we prefer our first representation as the more suitable for computability.

Example. Let $n = 3$, $m = 3$. $K = Z_2(\alpha)$ where α is root of $x^3 + x + 1 = 0$. $P(x) = b_0 + b_1x + b_2x^2$.

Code E: $(b_0, b_1, b_2) \rightarrow (P(0), P(\alpha), P(\alpha^2), \cdots, P(\alpha^6), P(1))$.

Binary translation of this code. To $f(x) = x^3 + x + 1$ we associate the difference equation

$$a_n = a_{n-2} + a_{n-3} \qquad (\text{for } n = 3, 4, 5, \cdots).$$

Choose $a_0 = 1$, $a_1 = 1$, $a_2 = 0$. Then

$$\{a_n\} = (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, \cdots).$$

$\{a_n\}$ has period 7, i.e., $a_7 = a_0$, $a_8 = a_1$.

$$0 = (0, 0, 0)$$
$$\alpha = (1, 1, 0)$$
$$\alpha^2 = (1, 0, 0)$$
$$\alpha^3 = (0, 0, 1)$$
$$\alpha^4 = (0, 1, 0)$$
$$\alpha^5 = (1, 0, 1)$$
$$\alpha^6 = (0, 1, 1)$$
$$1 = \alpha^7 = (1, 1, 1).$$

The message $(0, \alpha, \alpha^3) \rightarrow (P(0), P(\alpha), P(\alpha^2), \cdots, P(\alpha^6), P(1))$ translates into (via $P(x) = \alpha x + \alpha^3 x^2$)

(0 0 0 1 1 0 0 0 1)

$\rightarrow$ (0 0 0, 0 0 1, 1 1 0, 1 1 0, 1 1 1, 0 0 0, 0 0 1, 1 1 1).

This code is error correcting up to $(2^3 - 3 - 1)/2 = 2$ symbols.

REFERENCES

1. R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J., 26 (1950), pp. 147–160.
2. I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Trans. I.R.E., Prof. Group on Information Theory No. 4 (1954), pp. 38–49.
3. N. Zierler, *Linear recurring sequences*, this Journal, 7 (1959), pp. 31–48.